SAP Fiori for SAP S/4HANA –

SAP Fiori Security Design Fundamentals

*R*efer to the official SAP S/4HANA Security Guide in the SAP Help Portal. You can find this at SAP S/4HANA Product Page at https://help.sap.com/s4hana_op > Implement > Security Guide.

TLDR; *Just like a security guard ensures people can access a building to physically get to their office but not restricted areas; digital security needs to ensure users can do what they need to in the system and prevent them from doing something they shouldn't.*

Like a security guard who protects your physical workplace, security experts are there to safely enable access to your digital workplace

These are 10 fundamental principles to keep in mind when planning your security design for SAP Fiori for SAP S/4HANA:

1. User Experience must be prioritized over a technical approach to role design
2. Fiori business roles are composite roles (i.e. consist of one or more single roles)
3. SAP Fiori security is derived top-down from the business role
4. Have an "every user" role, e.g. the SAP Fiori Foundation User role
5. Start by mapping your custom business roles to SAP Business Roles

6. Where the SAP business role is too broad or doesn't cover your needs, create a custom business role
7. Where SAP Fiori apps do too much, use key user adaptation to create App Variants that limit the features
8. Where classic UIs do too much, use SAP Screen Personas to hide unwanted features
9. Consider separating out roles that assign search objects from roles that assign apps
10. Refine your data authorizations where needed

These are some other considerations that inform your security design:

11. You need to include key user roles in your security design
12. You need to include configuration roles in your security design
13. Adding launchpad content requires creation of custom technical catalogs
14. You need to understand the relationship between authorizations and launchpad layouts
15. Consider user provisioning goals in naming conventions
16. SAP_ALL cannot be used to grant access to SAP Fiori

IMPORTANT: If you have strict segregation of duties requirements, you may also need to consider additional components to manage these, such as SAP Access Control. While segregation of duties is beyond the scope of this blog post, as an initial starting point, you should look to avoid segregation of duties issues at the business catalog level, which is the lowest level of assignment of apps/UIs to roles. In our customer experiences, observationally most SAP standard business catalogs do not contain inherent conflicts. However, as rules and regulations can be different in different countries and for different industries, you should risk assess them for your conditions, for example using a ruleset.

Fundamental Security Design Principles of SAP Fiori

1. User Experience must be prioritized over a technical role design

Business outcomes matter more than technical role design – for both your business and your business users.

User Experience is critical to user adoption and usability. If your users find your system cumbersome to work with or full of restrictive security hurdles, that impacts on their desire to work with the system, and it distracts them from thinking about the work they have to do.

If you users are struggling to adopt or use your system, then your business cannot achieve their desired business outcomes that your system is there to support.

So achieving those business outcomes – by making sure your solution is easy to adopt and use – is and must always be your first priority.

It is possible to achieve adequate security without adverse impact to users.

You might think of the security role designer as like a bodyguard – you are there to work with your client (the business) to work out how to achieve whatever it is they want to achieve as safely as possible. You are not there to stop them doing what they want or need to do. Put your client first always!

2. Fiori business roles are composite roles (i.e. consist of a number of single roles)

Your composite role can assign single roles to control:

- **Access to the launchpad and launchpad features**
- **Access to apps and classic UIs**
- **Default layout (space)**
- **Access to search objects**
- **Access to data and actions performed on data**
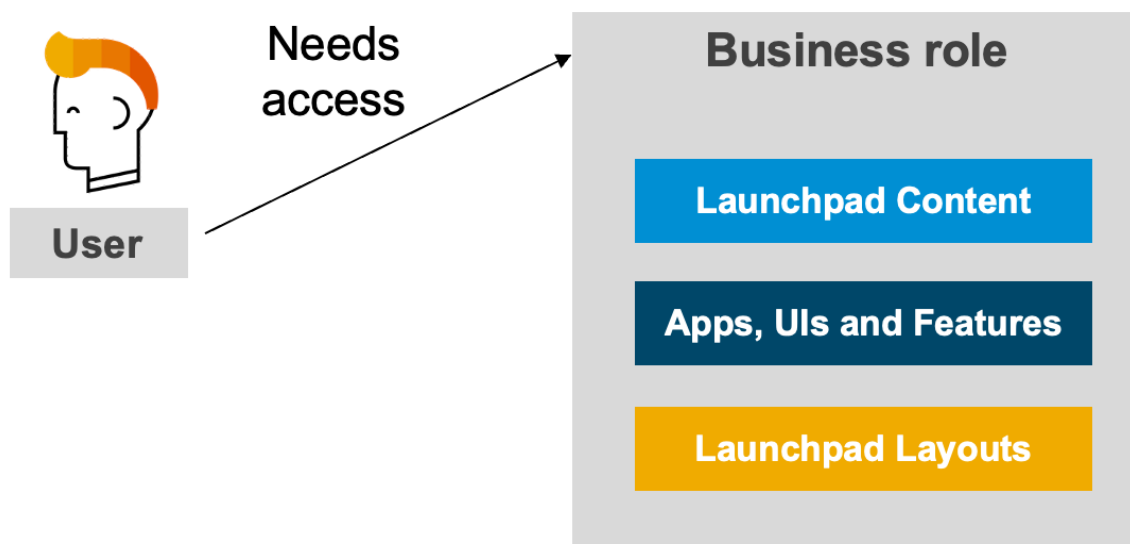
Users need access to SAP Fiori launchpad features, content, and layouts. This access is granted via their business role(s).

Technically in SAP solutions, composite Roles are optional but are encouraged to simplify user administration. While single Roles are used to provide authorizations.

SAP uses composite roles to model business roles within an organization. So SAP Business Roles represent the job of users and their related tasks. Examples of business roles include: Asset Accountant, Purchaser, Customer Sales Manager, Inventory Manager, Warehouse Clerk, etc.

SAP S/4HANA delivers more than 500 job-based templates – known as SAP Business Roles – which are working examples of how composite roles deliver the SAP Fiori user experience for a user who has role-specific tasks and responsibilities.

By convention SAP Business Roles have the prefix SAP_BR_.

SAP Business Roles can be found in the SAP Fiori apps library and in your system (in GUI transaction PFCG). Each role is named after the job, e.g.. General Ledger Accountant, with a matching technical id for the composite security role, e.g. SAP_BR_GL_ACCOUNTANT.

You can use the SAP Business Roles as a starting point to explore your SAP solution.

You are recommended to take a similar approach when creating custom business roles. Every organization has a certain set of such "personas" or "roles" within the various departments. The security team usually works very closely with the Functional team to identify these on project level.

Working together with the business ensures a shared understanding of the naming, intention, and purpose of each role, and the priority of the role with respect to business outcomes and strategic direction.

For example: Asset accountant, Purchasing officer, Factory floor supervisor, Customer Call Center supervisor, etc.

Usually, the most efficient approach is to map your custom business roles to the closest fit SAP Business Roles. Then copy the SAP Business Role and refine where needed to create your custom business role tailored for your organization's needs.

Refer to:

- SAP Fiori for SAP S/4HANA – Understanding SAP Business Roles
- SAP Fiori for SAP S/4HANA – Creating your custom business roles – the end-to-end process and video playlist

3. SAP Fiori security is derived top-down from the business role

Most permissions are derived automatically to the role, based on the business catalogs assigned to the role.

Business catalogs control the content available to a user from the launchpad.

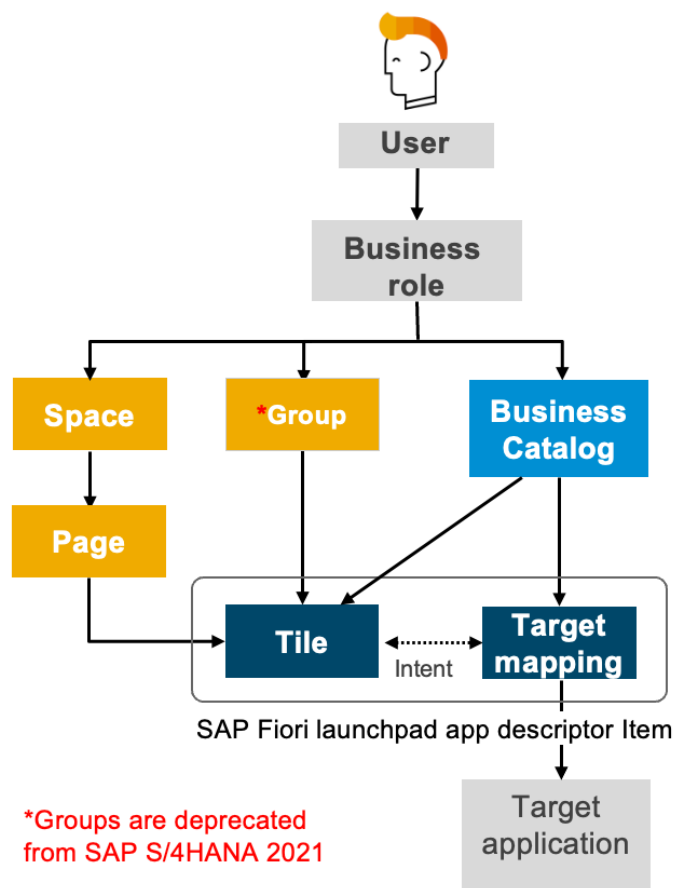**Tip:** Both business roles and business catalogs are client specific.

The single role that contains the business catalog(s), provides the authorization control and permission on application level. The business catalog also provides the logical intents that control the navigation between apps and UIs and the parameters passed.

Business catalogs are an independent collection of apps and UIs, that represent the apps/UIs that go together and should be assigned to a role together. The apps and UIs usually relate to the same Line of Business task and process. For example, an Overview Page app and the apps/UIs you navigate to from this app.

Usually, the business catalog collects around 2 to 20 related apps and UIs. Avoid creating large business catalogs as these are harder to reuse. Large business catalogs also increase the risk of creating a segregation of duties violation.

In practice the relationship between the business catalog and the apps within it is managed via intermediary references known as Tiles and Target Mappings. The tile controls the visual appearance of the entry point to the app, i.e. what appears on a standard tile, wide tile, flat wide tile, flat tile or link. The Target Mapping contains the details for launching the target app, for example which technical app id is launched using which UI technology, and which parameters are passed to the target app. The combination of a tile and target mapping is known as a SAP Fiori **launchpad app descriptor item**.

There is a loose relationship between the content and the layout, where a page reference a tile in the business catalog, when the tile needs to appear on a page. Not every tile needs to appear on a page. Tiles can also be visualized purely as navigational hyperlinks, for example: from search results; in Related Apps buttons; in list of links dialogs; or in jump-to targets of analytics.

Overview of the content and layout entities of a business role. Layouts are controlled via spaces and pages (which supersede groups). Content is controlled via business catalogs which collect tile and target mapping combinations known as launchpad app descriptor items. Pages reference tiles in the business catalogs.

Business catalogs can be assigned to one or more roles. In practice, most business catalogs are likely to be assigned to one and only one role.

There are also some mass maintenance tools you can use to assist mapping catalogs to create custom business roles, where needed.

Refer to:

- SAP Fiori for SAP S/4HANA – Combining business catalogs into custom business roles
- SAP Fiori for SAP S/4HANA – Mass maintenance of Business Roles for SAP Fiori launchpad

4. Have an "every user" role, e.g. the SAP Fiori Foundation User role

The Fiori Foundation role grants access to the launchpad itself and any common launchpad features for all users. Because this is a global role, you only add the base access you want all users to receive. This means your design includes giving every user a common Foundation User role in addition to one or more specific business roles.
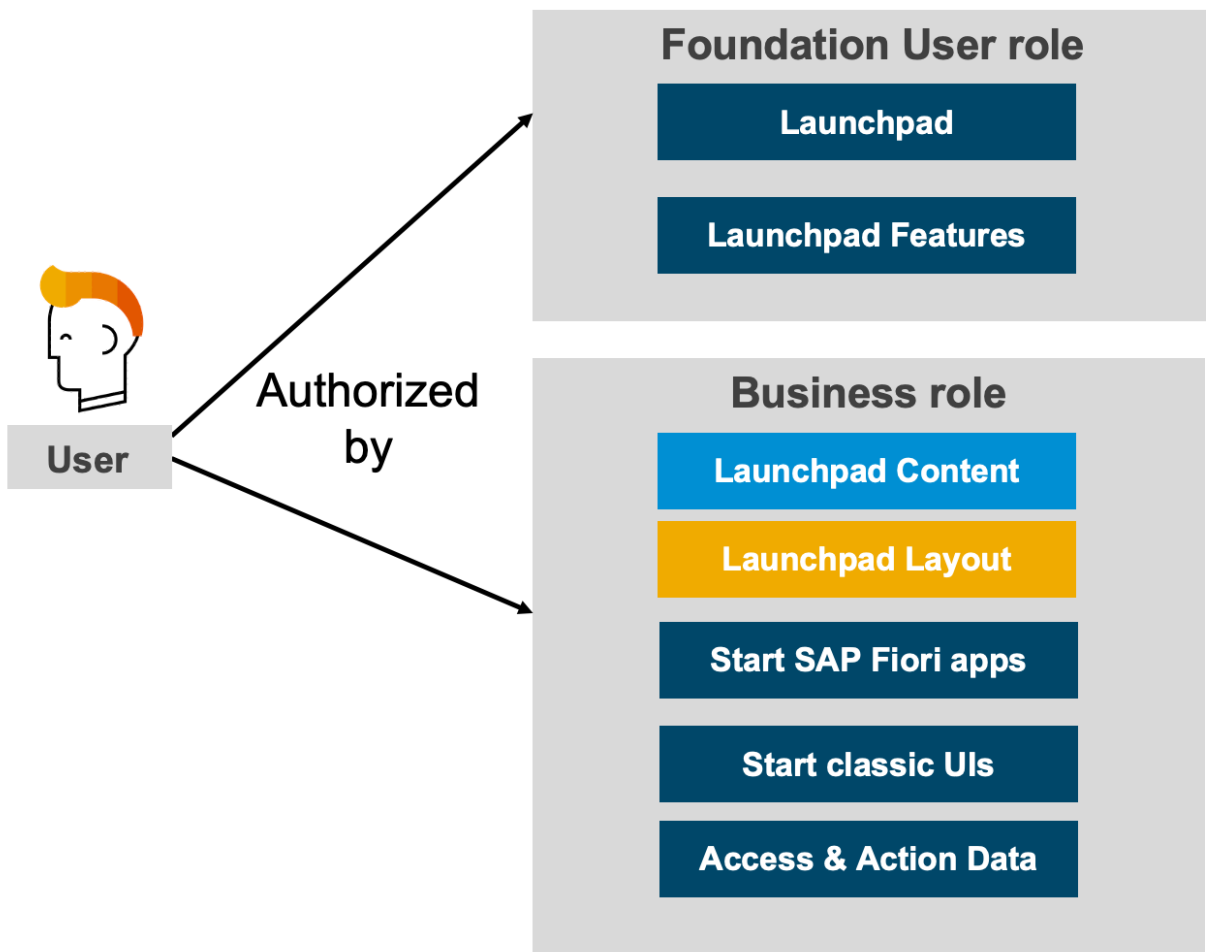
A user is authorized to access the launchpad and every user launchpad features by the Fiori Foundation user role. Their business role(s) grant access to role-specific content, layouts, start SAP Fiori apps, start classic UIs, data and actions on data.

By default, two initial Fiori Foundation Roles (Fiori Foundation User and Fiori Foundation Admin) are generated as part of task list SAP_FIORI_FOUNDATION_S4, task Generate Fiori Foundation Roles. You are recommended to use these as a starting point and adjust where needed.

Tip: If you wish, you can rerun the task lists or selected tasks of the task list when you upgrade your SAP S/4HANA release to update these roles to the latest capabilities for your target release.

For example: You might use your Fiori Foundation User role to grant access to the services needed for Search, Notifications, context-sensitive help, the launchpad itself, user defaults, personalization, App Support (e.g. to capture Authorization errors), etc.

Where you need to limit organizational data, then do that via a different single role. For example, put access to the search objects you can use in the Search into a different role.

You should also review the available Launchpad Configuration Parameters, as many of these can be used to turn on/off certain features globally. These can be viewed/adjusted in transaction /UI2/FLP_CUS_CONF. These settings are centrally managed by your UX Architect or IT team. Any changes must be discussed carefully so that the impact on users is understood. Any changes are applied immediately to all users.

Refer to:

- Launchpad Configuration Parameters in the SAP Fiori launchpad guide in the SAP Help Portal

5. Start by mapping your custom business roles to SAP Business Roles

This gives a first cut of authorizations that are likely to be relevant to the job and related tasks that a person needs.

A typical process is:

1. Extract the SAP Business Roles in scope.
2. Map to your target custom business roles.
3. Review the most likely UX to include in scope – this includes Fiori features (e.g. Search, Notifications), apps, and Intelligent use cases.
4. Once scope is decided, review the authorization matrix that will be used for building the roles.

There are several ways of deciding on scope. For example, using the SAP Best Practices Explorer procsss recommendations or the UX Value Goals content in SAP Activate.

Refer to:

- SAP Best Practices Explorer
- Introducing UX Value Goals
- Selecting apps by UX Value Goals
- UX Adoption as an iterative process
- Understanding the UX Adoption workshops
- UX Adoption – Why Select UX before Fit-to-standard

Within your solution, you can use the Launchpad Content Aggregator tool to audit the content of roles that you have created and any SAP Business Roles that you use as-is.

Refer to:

- SAP Fiori for SAP S/4HANA – 3 simple use cases for Launchpad Content Aggregator

Tip: The App Support tool can be used by users to identify missing authorizations to apps or UIs.

Refer to:

- App Support for the SAP Fiori Launchpad
- SAP Fiori for SAP S/4HANA – 10 health checks for the SAP Fiori launchpad

6. Where the SAP Business Role is too broad or doesn't cover your needs, create a custom business role

You can map your SAP Business Catalogs to your custom business roles.

It is very easy to refine custom roles by collecting catalogs.

Security experts also confirm this is generally a good approach to avoid/minimize Segregation of Duties (SoD) issues, although it is wise to double-check the contents of the catalog does not contain any SoD conflicts, where SoD needs to be strictly applied.

You can create your own custom business catalogs if you need to refine further – e.g. to remove apps you don't want at all, to add custom apps.

Refer to:

- SAP Fiori for SAP S/4HANA – Creating your custom business roles – the end-to-end process and video playlist

7. Where SAP Fiori apps do too much, use key user adaptation to create App Variants that limit the features

Each app is intended as fit for the tasks of a certain business role. The features of the app will reflect the intended task and audience. Before attempting to change the app, make sure you have understood the intended task and intended audience for the app, and confirm that it is a fit for your custom business role.

For example, the following apps all provide ways to count stock, but they are aimed at different tasks for different intended audiences:

- F2793 Pick by Cart for the Warehouse Operative
- F3340 Count Physical Inventory for the Warehouse Clerk
- F5563 Count Stock Ad hoc for the Retail Store Associate

- F3579 Count Products with RFID
- F1512 Count Stock for the Retail Store Associate

App Variants place a layer over the original app, and can be used to strip out certain features such as remove buttons, sections, etc.

You can create multiple **App Variants** for the same app, e.g. to create different variations of the app for different business roles. For example, you can use an App Variant to create a "display only" variant of a Manage app, by removing buttons that permit changes.

From a security authorizations perspective, App Variants are treated like a new app within your business catalogs and business roles.

Where key user adaptation is not enough, as a fallback, explore UI Adaptation at Runtime (developer technique) in the Business Application Studio.

Avoid copying apps as much as possible. A copied app is no supported by SAP, so the maintenance of a copied app is roughly equivalent to maintaining your own custom app created from scratch.

For an example of adjusting an app to remove features via Adapt UI, refer to:

- SAP Fiori for SAP S/4HANA – Creating your custom business roles – the end-to-end process and video playlist

8. Where classic UIs do too much, use SAP Screen Personas to hide unwanted fields/buttons/etc.

For classic UIs such as GUI transactions and Web Dynpro ABAP applications, SAP Screen Personas is the recommended tool to hide unwanted fields, tables, tabs, etc. This simplifies the transaction and avoids errors. In Screen Personas you create Flavors which are overlays to adjust the appearance and behaviour of the original classic UI.

SAP Screen Personas does not change the underlying behaviour of the original transaction. So from a security perspective, authorizations to limit data and activities within the UI should still be applied to all users of the classic UI, regardless of whether they are using the original UI or the UI with a SAP Screen Personas flavor overlay applied. The value of applying a SAP Screen Personas flavor is that it minimizes the opportunity to access unwanted data and features, while maximizing the task efficiency of the user.

Tip: As a general guideline, configuration options to limit features in the classic UI should be exhausted first before creating a Screen Personas "Flavor" to make further adjustments.

Where SAP Screen Personas is used, you will need to include in your Security Design

1. An administrator role for Screen Personas
2. Roles for key users to create Screen Persona Flavors

For business users, the link to the flavor is included in the business catalog by the Fiori administrator. For example, the Flavor is added as an additional parameter of the original classic UI. You may also need to include some permissions for accessing flavors in your Fiori Foundation user role

There is no license implication for using SAP Screen Personas, however the SAP Screen Personas software component needs to be installed.

Tip: For SAP S/4HANA Cloud, private edition customers, installing the software component would typically be done by your SAP ECS team, at your request.

9. Consider separating out roles that assign Search objects from roles that assign Apps

For example, if you want to create Line of Business collections of business objects for search to be assigned across multiple roles.

Search results will link to whichever related apps are logically assigned to the user.

As a general guideline, you should consider including the search object permission if the user has any app/Ui that uses the same Semantic Object. For example, where users are assigned app Manage Purchase Orders, they should also be able to use Search to find Purchase Orders.

A possible approach is:

- Include access to the OData Service for Search in your every user role, e.g. the Fiori Foundation User role
- Include the access to the Search Object in a Search role
- The data authorizations required for the search and the apps that are provided as links in the search results are then derived from the user's assigned business catalogs

Tip: Users often need to be able to further details of a search object, i.e. when using the hyperlink on the object id in the search results. By default the app launched from the hyperlink on the object id is identified via a Target Mapping with the same Semantic Object as the search object, and the default action **displayFactSheet**. So as part of your catalog design, you may wish to ensure roles with these search objects also have a business catalog containing a matching displayFactSheet target mapping for each search object.

Refer to:

- [SAP Fiori for SAP S/4HANA –Limit Search Object Access in Fiori Launchpad made easier](#)

10. Refine your data authorizations where needed

You will need to align with the business on data access requirements based on your:

- Enterprise model – company codes, plants, purchasing org, sales org, etc
- Information Classification/Handling – what is sensitive and must be restricted
- Organisational Structure – centralised vs decentralised

Default data authorizations are related to the OData Service and are managed using transaction SU24N. You can see the defaults delivered by SAP in transactions SU22. You can use transaction SU25 to adopt these during your initial system install and on upgrade of your SAP S/4HANA release.

Refer to:

- SAP Note 2798443 – SU24N: New dialog environment for authorization default value

This blog post gives an example of how to find the data authorizations you need for an app: SAP Fiori for SAP S/4HANA –How to restrict filter values in SAP Fiori apps

Other considerations for Security Design

11. You need to include key user roles in your Security Design

Key users are authorized to configure, adapt and extend apps on behalf of other users. They typically make these changes in your development environment – like any other configuration – and the changes are tested and transported.

For example,

- They may preset the default settings for filters, tables, and charts in apps as explained in SAP Fiori for SAP S/4HANA – New options for managing Views for filters tables and charts
- They may create analytics or configure intelligent use cases using some of the configuration apps listed in SAP Fiori for SAP S/4HANA – Yes you need SAP Fiori to Configure, Adapt and Extend SAP S/4HANA
- They may adjust the visibility of fields, buttons, sections, and tables using Adapt UI as explained in the SAP Fiori launchpad user guide in Adapting SAP Fiori UIs at Runtime – Key User Adaptation

Key user roles should be a composite role that includes:

- Key user capabilities to configure/adapt/extend your solution
- Regular business user role they impact (so they can see the impact of their changes)

Key user capabilities are critical to correct fit evaluation of apps, as they control visibility of fields, sections, tables, etc. within a SAP Fiori app. Some apps have more than 100 hidden fields available.

Key user capabilities also control use of custom fields, where needed.

You may need to consider different roles for tasks performed in non-production vs. production.

For more suggestions on how to approach such roles refer to:

- SAP Fiori for SAP S/4HANA – Granting Project Users SAP Fiori Launchpad Access

12. You need to include configuration roles in your Security Design

Whether or not you have designated key users, you will still need to assign SAP Fiori apps to configure extend and adapt your SAP S/4HANA solution for your functional teams and your administrators. For example to add custom fields, to configure workflows, or to configure certain outputs, such as advanced compliance reports.
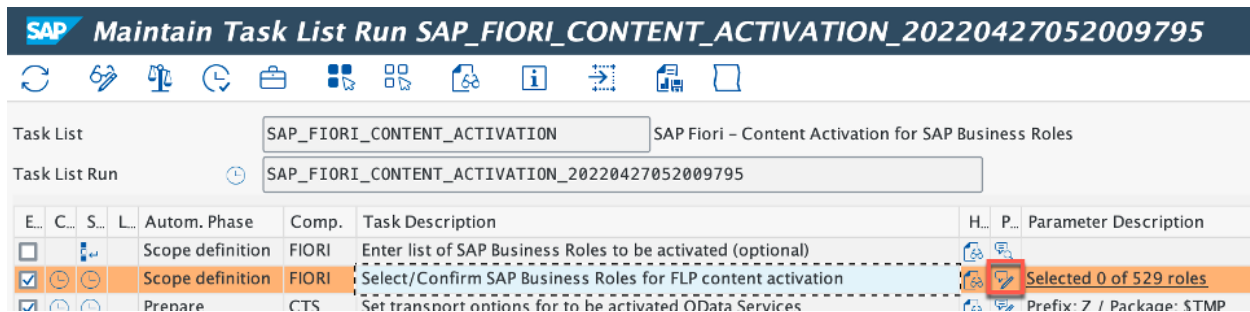
Refer to:

- SAP Fiori for SAP S/4HANA – Yes you need SAP Fiori to Configure, Adapt and Extend SAP S/4HANA

Most of these apps are in the SAP Business Roles:

- Administrator,
- Analytics Specialist,
- Business Process Specialist, and
- Configuration Expert – Business Process Configuration

Typically, you should copy these roles to the customer namespace and refine them as you do other business roles.

In the Task list manager, GUI transaction STC01, you can use the task list **SAP_FIORI_CONTENT_ACTIVATION** to generate these roles. You select the roles in task **Select/Confirm SAP Business roles for FLP Content Activation**, using the Fill Parameters icon.

Task list SAP_FIORI_CONTENT_ACTIVATION highlighting the task to select business roles
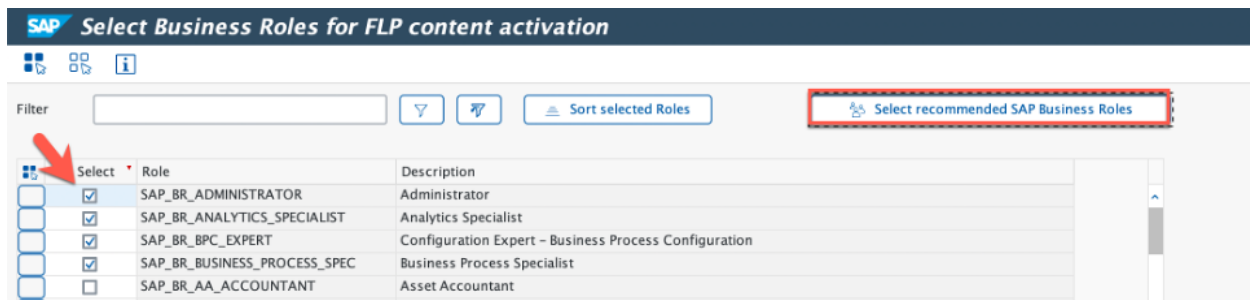
When in the role selection dialog, you can choose the option **Select Recommended SAP Business Roles.** This automatically selects the 4 configuration roles for activation. You save the selected roles and continue with the remainder of the task list as usual to execute the roles.

Role selection dialog highlighting the Select Recommended SAP Business Roles button

You will need to assign the generated roles to a user. You can use a generated test user as a quick option to get started by selecting the task **Create users with generated business roles** and completing the parameters to set a password and confirm your every user Fiori Foundation user role.
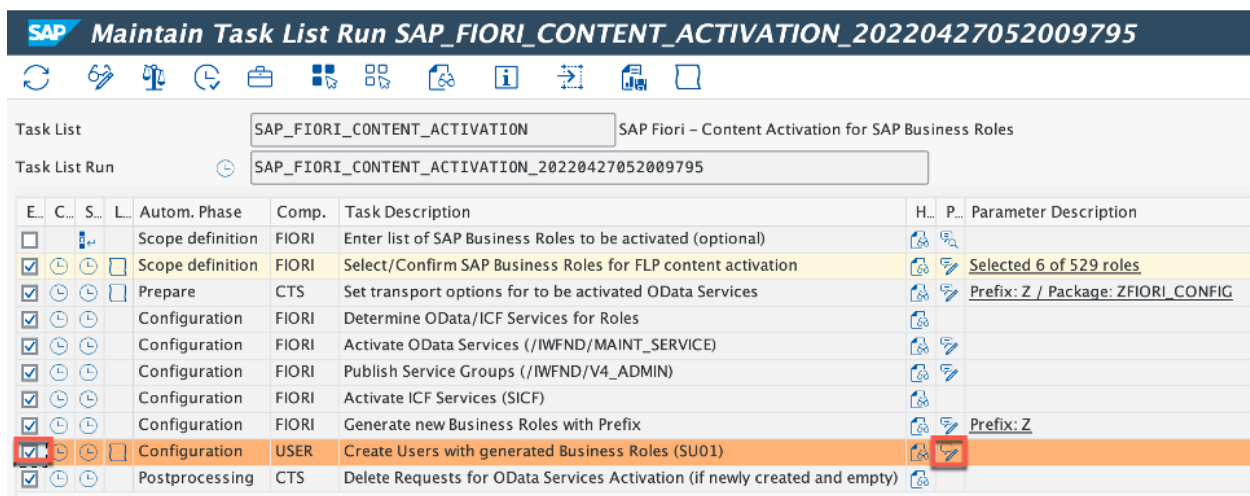
Task list SAP_FIORI_CONTENT_ACTIVATION highlighting the task to generate test users

You will also need the **Fiori Foundation Administrator** role to manage launchpad content and layout

The Fiori Foundation Admin role is generated as part of task list **SAP_FIORI_FOUNDATION_S4**, task **Generate Fiori Foundation Roles**. You execute the task list in STC01 and can see previous task list runs in transactions STC02. By default, it is called Z_FIORI_FOUNDATION_ADMIN.
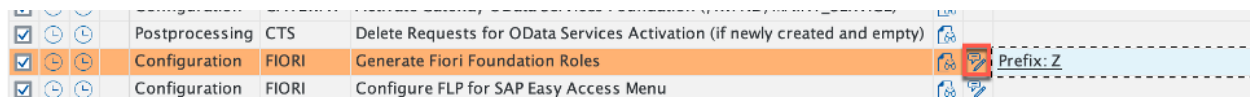
Task list SAP_FIORI_FOUNDATION_S4 highlighting the task Generate Fiori Foundation Roles

Tip: If you didn't generate the roles previously, you can execute the task alone by using the deselect all option, and then just selecting that task in the task list. Any dependent tasks will be automatically selected. You can also rerun the task list or selected tasks in the task list when you upgrade your SAP S/4HANA release.

IMPORTANT: You may need to consider different roles for configuration performed in development vs. related monitoring activities in your other environments (quality assurance, production, etc.).

13. Adding launchpad content requires creation of custom technical catalogs

Technical catalogs are cross-client and hold the settings needed to launch the app or UI, and any parameter mappings used when the app/UI is launched. Technical catalogs provided a layer of reuse to better manage and minimize launchpad content maintenance, particularly where tiles and target mappings are reused in multiple business catalogs.

You can find out more about Technical Catalogs in the SAP Fiori launchpad guide in the SAP Help Portal, in the sections Best Practices for Managing Catalogs and Setting Up Technical Catalogs.
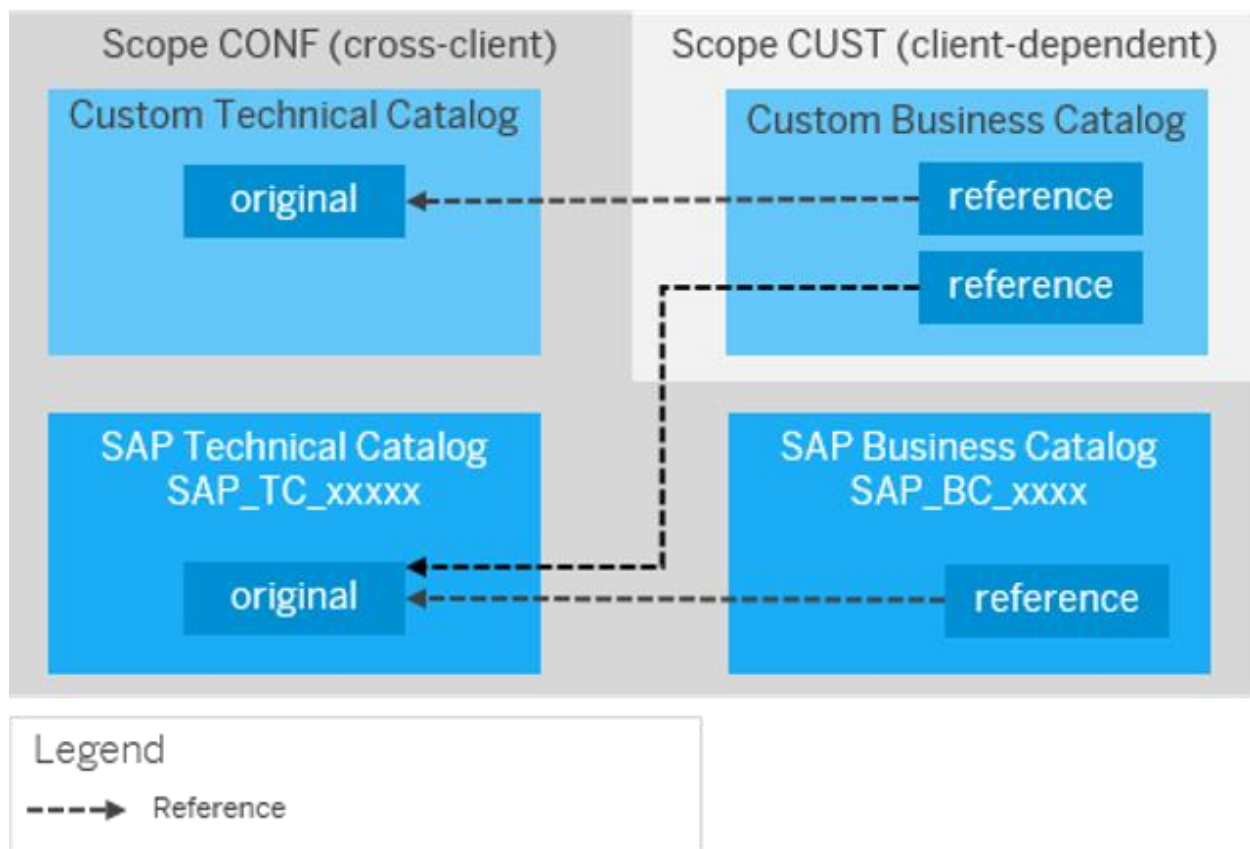

Illustration of the reference relationships between business catalogs that assign content to roles, and technical catalogs that hold the original tile and target mapping entries

When creating content in technical catalogs, the **Semantic Object** and action identify the matching tiles and target mappings.

IMPORTANT: You should use SAP delivered **Semantic Objects** as much as possible, as these automatically and dynamically include your custom content alongside related SAP delivered content.

For example, in search results, in smart link dialogs, in Related Apps menu buttons, in Jump-to targets of analytical apps, etc.

One or more business catalogs then reference the technical catalog entries at the client-specific level.

The business catalog is then incorporated into the business role.

When changing catalogs to add content, make sure the role and its authorizations is updated. For example, by using the program **PRGN_COMPARE_ROLE_MENU**.

While automation reduces the time needed for access to apps and classic UIs, you may still need to restrict some data values further, so make sure you consider this in your design.

14. You need to understand the relationship between authorizations and launchpad layout

Launchpad layouts do NOT have any impact on the content available to a user via the launchpad.

The only impact of layouts on the custom business role is the assignment of the space (top level of the layout) for that role to the role.

IMPORTANT: Regardless of what tiles are assigned to the layout, if the user does not have access to an app or classic UI they cannot launch it from the launchpad.

By default, if the user has no access the layout will automatically hide the related tile or link from the user. Knowing this can be particularly useful where your security design involves sharing certain pages across roles. You can even test the page against different role contexts using the **Preview** feature in SAP Fiori app F4512 Manage Launchpad Pages.

Where a user can see a tile or link and then sees an error message, this indicates that the app or UI has been partially assigned, and the authorizations need to be corrected.

The App Support tool is strongly recommended to assist with troubleshooting authorizations issues.

Refer to:

- App Support for the SAP Fiori Launchpad
- SAP Fiori for SAP S/4HANA – 10 health checks for the SAP Fiori launchpad

Within your solution you can use the Overview of Roles, Spaces, and Pages transaction **/UI2/RSP_LIST** to get an Overview of the Spaces and Pages assigned to Roles, and the tiles/links within them.

Within your solution, you can use the Overview of Roles, Spaces and Pages tool to analyze the layout of roles that you have created and any SAP Business Roles that you use as-is.

Refer to:

- Analyzing Space and Page Assignments in the SAP Fiori launchpad guide in the SAP Help Portal.

IMPORTANT: If you are on SAP S/4HANA 2020 or higher, you should focus on the spaces and pages layout mode and migrate to it as soon as possible. You should avoid the older groups layout mode used in earlier SAP S/4HANA releases. Groups mode is now deprecated.

From a security perspective, the spaces mode provides more flexible and efficient maintenance and support such as:

- Only the space needs to be assigned to the security role. Pages, sections, and titles are derived from the space. Changes in layout do not require any change to the security role.
- Pages can be assigned to multiple spaces, i.e. a page can be shared by multiple roles
- Pages cope automatically when there is any mismatch between role content and layout
    - Any tiles/links that the user is not authorized to use are automatically hidden from the user at runtime. Refer to SAP Note 3193445 – Console errors when no authorization for a tile in a Page
    - In SAP Fiori app F4512 Manage Launchpad Pages you can preview the pages against the different role contexts to which it is assigned. This lets you check what the user will see given the current content assigned to the page and the role.

Refer to:

- Migrating from groups to spaces and pages – Why, When, and Key Differences for Users
- **How to migrate from groups to spaces and pages**

15. Consider user provisioning goals in naming conventions

You will need to establish naming conventions for your business roles and business catalogs. Certain naming conventions impact:

- What users see in their Fiori launchpad, for example, in the App Finder
- How users navigate between launchpad features and apps
    - For example from Search results to related apps
- How users navigate from app-to-app
    - Here "app" includes SAP Fiori apps and classic UIs
- What key users and administrators can maintain
    - For example when distributing the maintenance of launchpad layouts (spaces and pages) to key users.

You will need naming conventions for:

- Business Roles – technical ID
- Business Catalogs – catalog ID and catalog name, as the name is visible to business users in the App Finder
- Technical Catalogs – catalog ID and catalog name. as the name is visible to administrators maintaining launchpad content
- Spaces – space ID and space name, as the name is visible to business users in their launchpad entry page
    - The space name does not need to be unique

- Pages – page ID and page name, as the name is visible to business users in their launchpad entry page
  - The page name does not need to be unique
  - A similar pattern of pages across analogous roles is recommended
- Custom apps – technical ID
  - You may also want to have your own equivalent of the SAP Fiori ID – forma g.F1511A, which provides an abbreviated id for uniquely identifying that is visible in the User Actions
- Semantic Objects – However, as a rule avoid creating Semantic Objects and use the closest fit SAP delivered objects. There are more than 3K delivered objects.

The following do NOT require naming conventions:

- Sections of pages – these are part of the pages and are not independent objects
- Tiles – these are identified by Semantic Object and action within catalogs
- Target Mappings – these are identified by Semantic Object and action within catalogs

16. SAP_ALL cannot be used to grant access to SAP Fiori

SAP_ALL should be avoided, even in Development.

WATCHPOINT: Be vigilant to make sure SAP_ALL is not "accidentally" or "temporarily" added to roles for SIT or UAT to get past issues. This can lead to disruptions in production when UAT has been completed while authorizations have still not been properly resolved.

Apps and tiles (e.g. to classic UIs) can only be assigned via business catalogs.

Even once apps and tiles are assigned, adding SAP_ALL is a risk for access to unauthorized data. This can even include access to some settings that are system-wide.

For further advice on managing project user roles refer to:

- SAP Fiori for SAP S/4HANA – Granting Project Users SAP Fiori Launchpad Access

Why Security Design matters

Security experts are usually looking to ensure users only have access to what they need. This means you may find their primary focus is on controlled enablement and protecting users from accessing features they do not need.

However, this also means security experts are critical to **ensuring business users have access to what they need to do their job every day**. This is particularly true in SAP Fiori where each business role is technically represented by a matching security role that controls the content and layout assigned to the user.

Think of a security guard monitoring a building – they are monitoring the building to make sure all the access points are working properly and not blocked or congested, just as much as they are monitoring to make sure no-one is doing something illegal or dangerous. In SAP Fiori, your security team are there to

make sure you have what you need to do your job, and they are also there to avoid you (or your company) getting into trouble accessing data or features you should not be using, such as personal data covered under GDPR.

IMPORTANT: In SAP Fiori for SAP S/4HANA, every business role has a matching security role. However not every security role is a business role. For more on this read SAP Fiori for SAP S/4HANA – Understanding Business Roles.

In other words, in SAP Fiori for SAP S/4HANA security controls the usual basics of tasks, data and actions, for example:

- Which apps and classic UIs are assigned to a user
- Which data they can view/maintain within apps and classic UIs
- What actions/features they can execute within apps and UIs.

Actions and features can include

- Actions specific to the app, e.g. Create Order, Reverse Journal
- Standard features such as app-to-app navigation, search, and notifications
- Key user features such as Adapt UI and creation of role-specific views for filters, tables, and charts
- And may also extend to intelligent features required by Machine Learning, Situation Handling, and Robotic Process Automation

Perhaps even more importantly, security authorizations control how users make sense of their day and what they can use to optimize their personal productivity including:

- Where and how they find their apps and classic UIs within the launchpad
- What features they can use within the launchpad, such as Search, Notification
    - This includes intelligent features such as Chatbots and Situation Handling
- Which navigations they can use to move from app to app or app to UI or feature to UI
- Which personalization features they can use to tailor their launchpad and apps to streamline their work. This includes, for example, features to:
    - Personalize their launchpad pages,
    - Personalize notifications and search,
    - Minimize data entry through setting Default Values, and Filter settings in apps
    - Minimize scrolling and clicking through setting default links in List of Links dialogs; setting default columns and sorting in tables; setting default dimensions, measures, and chart types in charts.

Next level security design with SAP Access Control

If you have strict segregation of duties requirements, you may need to take your security design to the next level with SAP Access Control. SAP Access Control is a part of SAP's Governance Risk and Compliance solution suite.

You can find information on how SAP Access Control integrates with SAP S/4HANA at Integration: Access Control with Fiori Apps for S/4HANA On-Premise

Yes, SAP Access Control supports risk analysis on SAP Fiori apps.

In SAP Access Control, rulesets are used to control access. Technically, the ruleset is a type of master data and the Fiori Apps are another action type.

Depending on system version, SAP Access Control offers business configuration sets (e.g. GRAC_RA_RULESET_S4HANA_ALL) for the SAP S/4HANA Rulesets. These are a global rule set for customers to use as a starting point to configure their own rules.

SAP Access Control also supports control of the other classic UIs that can be launchpad from the SAP Fiori launchpad such as SAP GUI transaction codes, Web Dynpro ABAP applications, and custom SAPUI5 applications (based on target mapping definitions). It also supports technical rules e.g. where you can define permission level rules at authorisation level.

SAP Access Control supports both Embedded and Standalone deployment modes of SAP Fiori front-end server.

Refer to:

- SAP Note 2652312 – Enhancement to S4HANA risk analysis to use same S4HANA ruleset even if Fiori Application is rendered from different system
- SAP Note 986996 – GRC Access Control- Best Practice for Rules and Risks

SAP Access Control even provides a few SAP Fiori apps of its own. Find out more at:

- SAP Fiori solution for SAP Access Control